UNITED STATES DISTRICT FOR THE
WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

v.

JOHN STUART,

Defendant.

21-CR-07-LJV-JJM

SUPPLEMENTAL MEMORANDUM OF LAW

INTRODUCTION

This Court heard argument on John Stuart's Objections and Appeal (Docket No. 100) on October 13, 2023. At the conclusion of the argument, this Court requested briefing on two issues: (1) whether a person has Fourth Amendment protections in his internet protocol (IP) address if that person was actively seeking to keep such information private, and (2) whether information gleaned by virtue of a Fourth Amendment violation can be used to establish probable cause in a subsequent application for a search warrant.

As to the first point, the defense noted at the argument that the Court may benefit from further briefing on the topic. That was request was granted. As to the second issue, the parties sharply disagreed. The defense maintained that the answer was "no." The government argued that good faith operated to rescue the improper evidence.

ARGUMENT

A. Tor users have a legitimate expectation of privacy in their IP addresses.

The Fourth Amendment provides, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. A two-part test determines whether an action violates the Fourth Amendment: (1) the person must have exhibited an actual (subjective) expectation of privacy, and (2) that expectation must be (objectively) reasonable. *Katz v. United States*, 389 U.S. 347, 361, (1967) (Harlan, J., concurring). Therefore, to establish a violation of one's rights under the Fourth Amendment, a defendant must first prove that he had a legitimate expectation of privacy in the place searched or the item seized. The defendant "must show that his subjective expectation of privacy is one that society is prepared to accept as objectively reasonable." *See California v. Greenwood*, 486 U.S. 35, 39, 1 (1988). Once a person establishes that he has met this test, the government must generally secure a warrant before any search can occur. *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 332, 338 (2009). "When an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize as reasonable, . . . official intrusion into that private sphere generally qualifies as a search and requires a warrant." *Carpenter v. United States*, 585 U.S. —, 138 S. Ct. 2206, 2213 (2018) (quotations omitted).

As a general matter, courts mostly agree that a typical internet user does not have a reasonable expectation of privacy in his or her IP address. That is because, like phone users who should know that by using their phone they are disclosing information to the phone company,

internet users "should know that [IP] information is provided to and used by Internet service providers for the specific purpose of directing the routing of information." *United States v. Ulbricht*, 858 F.3d 71, 96 (2d Cir. 2017) (quoting *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008)).

But that calculus changes when an internet user is actively seeking to keep IP address information private. This is precisely the purpose that Tor serves. Tor, an acronym for "The Onion Router," is an encrypted network that markets itself as a tool to "prevent[ ] people from learning your location." *See* Tor Project: Anonymity Online, https://www.torproject.org (last visited 12/1/2023). Users of Tor do not voluntarily turn over their information to third parties; rather they actively seek to keep that information private, and it is only through advanced hacking schemes – schemes that are only available to major state actors deploying sophisticated technology – that those IP addresses can be uncovered.

As the Eleventh Circuit has found, "that [the defendants] used Tor to download child pornography is important because it takes this case out of third-party-doctrine land." *United States v. Taylor*, 935 F.3d 1279, 1285, n.4 (11th Cir. 2019) (citing *Smith v. Maryland*, 442 U.S. 735 (1979)). The *Taylor* court expertly explains: "Instead of traveling along the equivalent of 'public highways' (by browsing the open internet) or leaving the equivalent of a calling card at each website visited (as with a normal internet search), Tor users purposefully shroud their browsing, such that they have a reasonable expectation of privacy in their online 'movements.'" *Id.*

While a small handful of district courts have found that Tor users do not have a

reasonable expectation of privacy in their IP addresses[1], those decisions are not binding, not well reasoned, and were issued before the Supreme Court decided *Carpenter* in June 2018.

In *Carpenter*, the Supreme Court recognized long-standing law that "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected," and it further rejected the "voluntary exposure" rationale of the third-party doctrine for cell site data. 138 S. Ct. at 2217, 2220. The Court reasoned:

> Cell phone location information is not truly "shared" as one normally understands the term. In the first place, cell phones and the services they provide are "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily "assume[ ] the risk" of turning over a comprehensive dossier of his physical movements.

Id. (internal citations omitted). That logic not only applies here, but it applies with greater force where, as here, the user takes affirmative steps to prevent the "sharing" of private data that, like cell phone location data, is logged simply by dint of powering up an internet browser.

In 2023, using the internet is a requirement of everyday life. Tor users – and anyone who opts for privacy in their internet browsing – understand that their IP address provides an intimate window into the user's private life, revealing not only his particular movements, but

---

[1] U*nited States v. Matish*, 193 F. Supp. 3d 585, 615 (E.D. Va. 2016); *United States v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *7 (W.D. Wash. Jan. 28, 2016); *United States v. Farrell*, No. CR15-029RAJ, 2016 WL 705197, at *2 (W.D. Wash. Feb. 23, 2016).

through them his "familial, political, professional, religious, and sexual associations." *See Riley v. California*, 573 U.S. 373, 396 (2014).

Accordingly, this Court should conclude, as the 11th Circuit did in *Taylor*, that a Tor user has a reasonable expectation of privacy in his IP address and that any warrantless search leading to disclosure of that IP address results in a Fourth Amendment violation.

B. This Court must hold a hearing to determine whether the search shocks the conscience, as well as to determine the amount of U.S. involvement and cooperation in the unconstitutional search.

Although the Fourth Amendment and its exclusionary rule generally do not apply to the law enforcement activities of foreign authorities acting in their own country, the concepts do apply where (1) the conduct of foreign officials in acquiring the evidence is so extreme that it shocks the judicial conscience, and second, (2) where U.S. cooperation with foreign law enforcement officials may implicate constitutional restrictions. *United States v. Getto*, 729 F.3d 221, 228 (2d Cir. 2013).

This Court cannot answer these questions without a hearing. As an initial matter, the prosecution in this case has claimed that it does not know how the hidden IP address was recovered. The government cannot, therefore, assure this Court that the manner in which it was uncovered would not shock the conscience. It is still unknown how the IP addresses were deanonymized – an ability that only nation states appear to have. To this point, the prosecution is only saying that the [redacted] provided a "tip" to the United States that certain IP addresses accessed certain Tor websites.

Second, we now know that the United States government was more than a passive recipient of a generous tip, despite the misleading nature of the search warrant application meant to leave this impression. As noted in previous briefing, there was long-standing

collaboration between, at least, [redacted], the [redacted] and the US. (*See Objections*, at pp. 13-16; Docket No. 100). Indeed, new facts demonstrating this collaboration continue to be unearthed.

The National Crime Agency, the law-enforcement arm of the [redacted] government tasked with investigating online crimes, code-named their investigation in this matter Operation or Project "Habitance." According to the [redacted], "[redacted] is the [redacted]'s project tackling child sexual exploitation offending on the dark web . . . Working with partners, the [redacted] has identified a significant number of unique global internet protocol (IP) addresses on dark web sites; at least 5 percent of these IP addresses are believed to be in the [redacted]." National Crime Agency, An inspection of the National Crime Agency's criminal intelligence function, p. 11 (July 2020) (attached as Ex. A).

At least one Homeland Security Agent, Gregory Squire, was deeply involved in that operation. Indeed, Agent Squire drafted one of the first – if not *the* first – affidavits in support of a criminal complaint charging an American with crimes associated with this operation. *See United States v. Bateman*, 20-CR-10012 (D. Mass.) (affidavit attached as Ex. B). Agent Squire has a Linkedin account in which he highlights an award bestowed on him by [redacted]. (Attached as Ex. C).[2]

It bears repeating that the warrant application leading to the search of Mr. Stuart's home is drafted to leave the impression that the U.S. was not involved at all; that they were the passive receipt of a lucky tip from a "foreign law enforcement agency." The government to

[2] The Director General is senior-most position in the [redacted]. He "takes charge of the [redacted]'s 6000 officers based in the [redacted] and overseas, and is responsible for setting the Agency's operational priorities, ensuring it is operating effectively, and shaping the entire [redacted] law enforcement response to serious and organised crime."
[redacted]

this day continues to assert that this was a case of "one-way information sharing" where the U.S. simply received information from the [redacted]. (Gov. Resp., at 19; Docket No. 105.) The defense's investigation reveals that to be false. Agent Squire was so intimately involved in the operation that the leader of this "foreign law enforcement agency" awarded him a commendation. Homeland Security (HSI) agents do not get commendations for passively receiving information; they get commendations for having a pivotal role in acquiring it. This fact alone establishes at least enough to warrant a hearing on the extent of the cooperation, the degree to which the [redacted] was an agent of the United States, and the nature of the investigation that led to the deanonymizing of Mr. Stuart's and thousands of others' IP addresses.

If more were needed, the United States Department of Justice itself touts among its "accomplishments" that it continues to "*lead and coordinate strategic enforcement operations* and/or prosecutions including those involving Arlan Harrell, John Brinson, Moises Martinez, and Keith Lawniczak who were active members of several Tor-network-based child exploitation websites, including '[redacted],'" the very website at issue in this case. *See* DOJ Performance Budget FY 2024 Congressional Submission, p. 29 (attached as Ex. D) (emphasis added).

Finally, documents recently received via a Freedom of Information request in a related case – *United States v. Sanders*, 20-CR-143 (E.D. Va)[3] – reveal the United States was sharing information with law enforcement partners in Germany relative to its investigation into this server even before the U.S. claims to have received the "tip" in August of 2019. Agents in the United States are discussing their operation with Germany in email exchanges dated June 13,

[3] Zackary Sanders was accused of accessing the same server – and was allegedly located as a result of the same "tip" from the [redacted] – as John Stuart.

June 14, June 20, June 21, and June 24 of 2019. (FOIA Response, attached as Ex. E, pp. 3-11.). On June 24, 2019, for instance the Chief of the Federal Criminal Police in Germany emailed a redacted HSI agent, saying "good job! The report will be useful for us." (*Id.*) This is not a one way street.

Other emails released in this batch demonstrate that at least as early as 2018, HSI and the FBI were working together on projects they called "good listener" and were emailing documents about "guard research." (*Id.*, at p. 24) In the world of Tor, the entry node is often called the guard node; it is the first node to which the Tor client connects. One email purports to show how "good listener" actually works, with sections on "Background" and "Methodology." This document is dated September 2018, well before the United States claims to have gotten a lucky "tip."

It must also be noted that in the FOIA response cover sheet, HSI indicates that it was providing only 71 (heavily redacted) pages. Another "935 pages have been temporarily set aside as a potential future supplemental production, pending confirmation of the existence of a court seal on those documents." (*Id.*)

Among the 71 redacted documents that were provided (only 7% of the total production that HSI itself deemed relevant), is an email chain dating back to July 1 of 2019 where FBI and HSI agents are discussing a draft search warrant affidavit "that has not been signed off on yet." (*Id.*, pp. 70-71.) This draft affidavit, it appears, eventually becomes the boilerplate affidavit ("Tor Op Go By," in their verbiage) that has been used in search warrant applications like the one for Mr. Stuart across the county. This is critical because the affidavit was being drafted *before* the U.S. received the "tip" in August of 2019. Although seemingly all names have been redacted, Agent Squire, who received the award from the [redacted] received an email

about the affidavit. (*Id*., p. 23).

The government still wants the defense and this Court to believe this tip was a "one way street." It was nothing of the sort. In its own words, United States law enforcement is "leading and coordinating" enforcement operations into the website that Mr. Stuart is accused of visiting. A United States law enforcement officer has received an award for work done on the very operation in the [redacted] where the deanonymization is alleged to have occurred. The United States admits that it played a critical role in uncovering the server that hosted the website. The U.S. is working on projects to uncover Tor users – and even drafting search warrant affidavits – well before the "tip" was received. All along, the U.S. was actively providing information to other countries. Despite all this, the government continues to assert that it did nothing more than receive a "tip," and that notions of agency or joint venture are mere "speculation." These government assertions can no longer be countenanced. Rather, it is becoming more and more clear that the warrant application was intentionally drafted in a manner to conceal the United States' very active role in this operation – likely in an effort to avoid having to disclose the constitutional concerns that a hearing would reveal.

C. Good faith.

The government has argued that good faith saves the warrant, in part because TFO Hockwater did not know that he was misleading the court. But the government cannot conceal its bad acts by trotting out a straw man to do its dirty work. TFO Hockwater applied for the search warrant and is therefore charged with knowledge of the investigation that led to the application. *See, e.g.*, *United States v. Bin Laden*, 397 F. Supp. 2d 465, 481 (S.D.N.Y. 2005), aff'd sub nom. *In re Terrorist Bombings of U.S. Embassies in E. Afr.*, 552 F.3d 93 (2d Cir. 2008) ("[I]t is clear that the investigating case agents on a particular prosecution are part of the

prosecution team."). *See also, e.g., Kyles v. Whitley*, 514 U.S. 419, 438 (1995) (rejecting the argument that a state prosecutor "should not be held accountable ... for evidence known only to police investigators and not to the prosecutor."). Surely a police officer cannot unlawfully break into a man's home, ransack the house, find contraband, and then tell a second officer only that contraband was found, all so that the second officer can apply for a warrant based on the recovered contraband without knowledge of the first officer's unlawful actions. Indeed, such a scheme would constitute the intentional misleading of the magistrate court – the opposite of good faith.

The government also seemed to suggest at oral argument that good faith saves the search despite any antecedent Fourth Amendment violation because the warrant itself acts a buffer against those violations. The existence of the warrant, in other words, cleanses any prior Fourth Amendment violation. This is inaccurate. The Supreme Court decided long ago that "in order to make effective the fundamental constitutional guarantees of sanctity of the home and inviolability of the person . . . . evidence seized during an unlawful search could not constitute proof against the victim of the search." *Wong Sun v. United States*, 371 U.S. 471, 484 - 485 (1963) (internal citations omitted). Information gleaned in violation of the Fourth Amendment cannot be used in a subsequent application for a warrant.

Finally, good faith does not apply in general in this case because "the judge in issuing [the] warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth." *United States v. Leon*, 468 U.S. 897, 923 (1984) (citing *Franks v. Delaware*, 438 U.S. 154 (1978)). As argued above, an FBI or HSI agent did not walk into his office one day to find a "tip" on his chair from an FLA. Rather, the U.S. was involved from the very beginning, it led the operation and

cooperated with other foreign law enforcement agencies, and, at its conclusion, a U.S. agent received an award for his work. This is a far cry from the information presented in (and omitted from) the Hockwater application, and it is at least sufficient to warrant a hearing on whether the assertion "that U.S. law enforcement personnel did not participate in the investigative work which FLA identified the IP address provided by FLA" was a fully or even partially truthful one. (Hockwater Application, ¶ 26). At the very least, a hearing is necessary to determine the extent to which the application was misleading.

CONCLUSION

This Court should suppress all the evidence obtained as a result of the search warrant, or order a *Franks* hearing based on the omissions and misrepresentations contained in the Hockwater application.

Dated: Buffalo, New York
December 1, 2023

Respectfully submitted,

/s/ Jeffrey T. Bagley
Jeffrey T. Bagley
jeffrey_bagley@fd.org
Assistant Federal Public Defenders
Federal Public Defender's Office
300 Pearl Street, Suite 200
Buffalo, New York 14202
(716) 551-3341
Counsel for John Stuart